REMARKS

Applicants respectfully request reconsideration of this application as amended.

In an effort to overcome the outstanding 35 U.S.C. § 101 rejection, Claim 14 has been amended to recite the terminal has a first computing means with a computing capacity greater than a computing capacity of the verifier entity. Claim 14 further recites electronic communication means enabling communication between the prover entity and the verifier entity. Amended Claim 14 is thus directed to a concrete useful solution at least because of the second computing means having lower computing capacity than the first computing means (See the specification, at least on page 2, lines 5-13). Accordingly, Applicants respectfully submit that Claim 14 is in full compliance with 35 U.S.C. § 101.

Regarding the art-based rejections, and in particular the Kocher reference, the Office Action asserts that the technical solution of the present invention is anticipated with reliance on disparate paragraphs of Kocher. The relied on paragraphs each recite a specific teaching relating to a complex method for implementing RSA for use in a cryptographic system. It is well established law that a prior art reference must be considered in its entirety, i.e., as a whole. Furthermore, the mere fact that one could rearrange specific teachings to meet the terms of the claims is not itself sufficient for a proper rejection.

In Kocher, an RSA encryption operation is used to produce encrypted messages (See Fig. 3) and an RSA decryption operation is used to recover the encrypted messages. As suggested by Kocher, for example in the claims, the method can only be performed within a smart card.

In contrast, independent Claim 14 includes the feature, which is performed by the verifier entity and thus has higher computing capacity, of performing at least one modular reduction by utilizing the pre-validation value.

In contrast, Kocher teaches that decryption operation (or signing) comprises (with reference to column 17 lines 39-40) of the following operations which are performed at the level of *the verifier* (e.g., in a smart card):

> receiving the input message C by the modular exponentiator of the verifier (See Fig. 3) and col. 17, lines 30-33;
>
> blinding the obtained value by computing $C' \leftarrow (C)(B_i) \bmod n$ (See column 17, lines 32-40); and
>
> computing the blinded result as M' (See column 17, line 45).

Applicants respectfully submit that Kocher at least does not teach or suggest using the first computing means for calculating at the level of the prover entity a pre-validation value representing at least a quotient of a modular calculation. Moreover, Kocher does not teach or suggest a communication of a specific pre-validation value from a prover entity of a higher calculation capacity to a verifier entity of lower calculation capacity.

Independent Claim 14 is thus patentably distinguishable from Kocher. The remaining references fail to overcome the deficiencies of Kocher.

Thus, in that none of the cited references, taken either alone or combination, teach or suggest each and every feature as recited in the claims, the claims are patentably distinguishable therefrom. An early Notice of Allowance is respectfully solicited.

Should the Examiner believe that any further action is necessary to place this application in better form for allowance, the Examiner is invited to contact Applicants' representative at the telephone number listed below.

The Commissioner is hereby authorized to charge to Deposit Account No.

50-1165 (T2146-906752) any fees under 37 C.F.R. §§ 1.16 and 1.17 that may be required by this paper and to credit any overpayment to that Account. If any extension of time is required in connection with the filing of this paper and has not been separately requested, such extension is hereby requested.

Respectfully submitted,

By:_____
Edward J. Kondracki
Reg. No. 20,604

Jason H. Vick
Reg. No. 45,285

JHV:cbt

Miles & Stockbridge P.C.
1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
(703) 903-9000

March 30, 2006